The Security Blanket

Issue 15, May/June/July 2003

Keeping I.T. Secure.

In This Issue:

Feature Articles

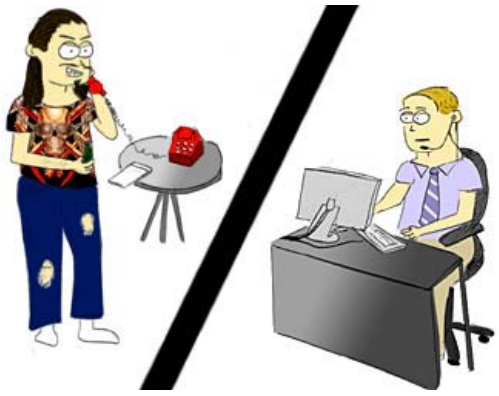
Social Engineering: The Often Unnoticed Attack

As the number and complexity of technical attacks on organizations' computer networks has increased, the use of countermeasures to thwart these attacks has increased, as well. Network security is now taken very seriously. As a result, the use of a technique called social engineering is becoming much more prevalent in attacks upon computer networks, as it is an attack upon what is often the weakest link in an organization's computer security: humans.

Simply put, social engineering is the attempt by attackers to gain access to data that they are not authorized to have by gaining the trust of an individual inside the organization being attacked. Once trust is established, this individual reveals the desired information to the attacker. This information is then used to further an attack upon the organization.

Social engineers use many different methods to establish trust and gain access to the desired data. As a result, social engineering attacks often go unnoticed by those being attacked. However, attacks generally begin with the attacker obtaining some information about an organization to be attacked. This information is collected in numerous ways.

One of the ways it can be obtained is by contacting members of an organization and asking seemingly mundane questions. This contact may be in the form of a phone call or various forms of written communication, most notably e-mail. The data also may be obtained from many other sources including press releases, websites, eavesdropping, or an organization's garbage. In any case, the data gleaned from these sources is then used to gain the trust of someone within the organization.



This is generally accomplished through the attacker posing as someone who is authorized to have the data the attacker is looking to obtain. The attacker may pretend to be a member of the organization who has forgotten their password, a hardware vendor looking to see if an organization is satisfied with current computer-related products, or any number of other people. The attacker will use the information they have obtained to make their claim of being someone authorized to have access to the desired data believable.

The member of the organization whose trust has been gained by the attacker will then give the attacker the desired data, as if the attacker were the person they are pretending to be. The attacker then uses this data to compromise some aspect of the organization's computer network with the goal of data theft, data destruction, identity theft, network disruption, or some other illicit end.

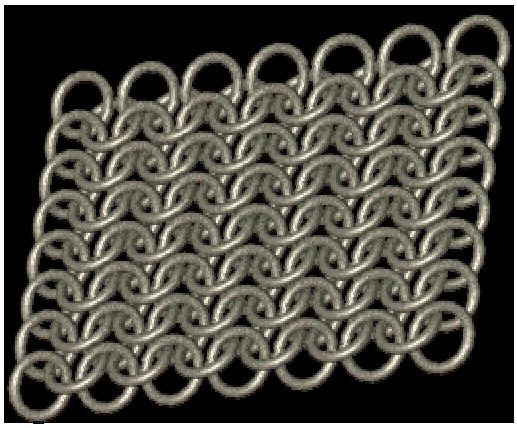
While it is not possible to completely defend against social engineering attacks, simple methods do exist to mitigate the chances of the attacker being successful. Some easily implemented defenses are:

- **Information Distribution** - Policies must be in place to deal with the distribution of information concerning computing resources within an organization. Employees must know who it is appropriate to give information to, and what information can be given to them.

- **Identity Verification** – In the event that employees are asked to reveal sensitive information, they must know how to verify that the person requesting information is who they say they are. Procedures for identity verification must be put into practice. Employees also need to be aware that no matter who is requesting the information, be it a fellow employee or a higher-up in the organization, the requester's identity must be verified. Furthermore, management must endorse the policy that no negative repercussions will result from challenging a person's identity.
- **Publicly Available Information** - Information available to the public about employees and computing resources should be kept to a minimum, as the less information social engineers have to work with the less likely they are to succeed.
- **Printed Material** - Any printed material deemed to contain sensitive information must be properly disposed of (i.e. shredded) in order to eliminate the possibility of attackers gaining information by going through an organization's garbage.
- **Visitors** - Visitors to an organization should be clearly identified and restricted to areas free of sensitive information. Employees should also be aware of their presence. This helps to prevent attackers from visiting an organization and obtaining data to be used in later social engineering attacks.

While the above defenses are by no means a complete list, they are a starting point for securing an organization against social engineering attacks. The creation and implementation of policies relating to these defenses will make an organization relatively secure against social engineering. However, employees need to be aware of the necessity of following policies concerning social engineering and the significant danger that this type of attack presents in order for these policies to be effective.

As a result, education is the key to implementing an effective defense against social engineering. Employees must be involved in an educational program designed to keep them up to date on new policies and social engineering attack methodologies. Only once all members of an organization are educated regarding their responsibilities in preventing social engineering attacks can an effective defense be realized.



An organization's defenses against social engineering attacks are only as strong as the weakest link in the organization's computer security.

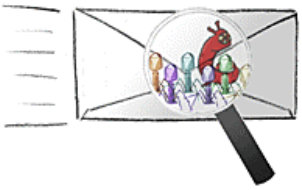
~Theo Peterson
ITD Intern 2003

Return to Table of Contents

Incoming! - Or: How I Learned To Stop Worrying and Love Email

Email. It's pervasive in the modern business world. Heck, it's pervasive in our home lives, too. It's incredibly convenient and quick (at least for those of us who remember sending actual *letters*) and it helps us communicate with, potentially, billions of people.

Ah, yes, there's the rub. Because not only can your friends email you, everyone with an email address can send you messages, too. Want to send someone flowers? Make more money? Enlarge your… portfolio? Well, eventually you'll get the information to do these things, because the volume of spam (unsolicited email solicitations) continues to rise. Yes, it is true that states, the federal government, and many businesses and special interest groups are fighting against spam's pervasiveness, and they might be able to curb the beast in time. But you can also help yourself by not giving out your email address to every business that asks for it. Whenever you share your address with companies it has the potential to be sold for marketing. Examine registration, license, and subscription notices carefully – you can often request to be kept off marketing lists.



One other sad truth about email is that it is the primary method of spreading malicious code – viruses, worms, and Trojan programs. I once was told (probably by my Dad) that whatever you own you have to take care of. Though I'm sure he was referring to my collection of toys that were scattered across the living room floor, his words really are sage advice for the information age. Every email user has a responsibility to protect themselves and their system against viruses and the like. Use anti-virus programs and keep them updated - they are a tremendous help in combating malicious code. Equally important, be aware of the issues and behave in a secure manner. Don't open attachments from unknown sources, don't forward spam, don't send confidential information via email without encryption, and don't click on those intriguing links in unsolicited emails. They usually don't take you to where you want to go.

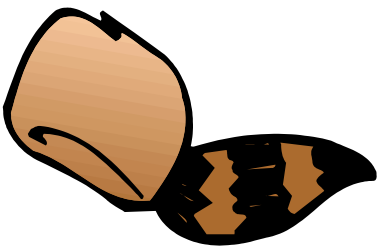
Email. It's a tremendously useful tool, and a wonderful communication device. But it also has its pitfalls. Use it wisely and take care of it, or you may find yourself facing some of the darker, more unfortunate aspects of the information age.

William Hubbard
DAS ITE, ISO

Return to Table of Contents

Current Activities

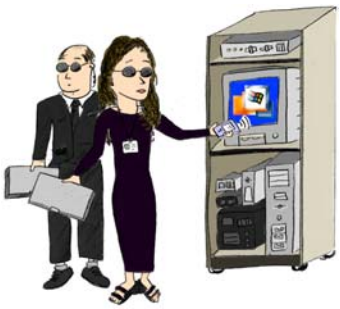
There so much going on that sometimes it feels like we're at the Alamo… departmental reorganization, policy development, vulnerability assessments, intrusion detection, staffing changes, ICAT development, K-12 Security Awareness Outreach, and the list goes on!



Information Security Office Service Offerings

Are you looking for security services? Interested in a vulnerability assessment on your systems? Need help developing your agency security policy? Need help with a security incident? Check out the ISO Service Offerings!

Visit the **ITD Billable Rates** web page for a complete listing of Security Service Rates. (Security Services are listed in the last quarter of the web page.)



- Security Consulting
- Vulnerability Assessments
- Physical Security Vulnerability Assessments
- Network-Based Intrusion Detection System
- Enterprise Business Continuity
- Incident Response
- Test Lab
- Awareness Briefings
- Enterprise IT Business Continuity

Information Security Officer Distribution List

The Information Security Office has a distribution list with which we can easily send out security mailings to security contacts within the State of Iowa. Mailings include the Security Blanket, Security Quickies, Lunch & Learns, Security Alerts, Daily News and Virus Reports, security events, or other announcements. Some contacts also disseminate the ISO mailings to their departmental personnel. If you are interested in being included in this distribution list, drop a note to Security Awareness.

If you would prefer to only get the Daily News and Virus Report, which is sent out every business day, send the note with this subject heading: Security Awareness.

Security Awareness Tutorial

The Security Awareness Tutorial (SAT) is an online/CD-ROM based training course that covers security topics like Confidential Information, User Accounts and Passwords, Workstation Security, Malicious Code (Viruses, Trojans, and Worms), Laptops, and Modems. It is divided into separate lessons, so you can complete the lessons at different times if needed.

The SAT is currently being used by the Department of Administrative Service – Information Technology Enterprise (DAS ITE – hey, that's us!) and other Enterprise departments for security awareness training. Because the Information Security Office has Enterprise-wide responsibilities, the SAT is also available to State of Iowa Enterprise

agencies at no charge. In addition, the SAT is available to non-Enterprise agencies and non-State of Iowa organizations as well, for a licensing fee.

For more detailed information such as system requirements and course content you can visit http://www.itd.state.ia.us/security/education.html#tutorial. Contact William Hubbard if you have questions regarding the SAT content, and Cory Oelberg for access to the course.

OTHER ACTIVITIES

Enterprise Security Website

The ISO site contains Security Awareness Resources, Operational Services, Policies, Procedures, Recommended Reading, and Mobile News, and Industry Best Practices. It's a free resource of Enterprise and DAS-IT security information.

Educational Extras

Extra resources are available here for State of Iowa security awareness efforts and home personal computer security.

Information Security Outreach

In an effort to assist with the federal security awareness outreach effort and to aid state employees, security awareness materials are being offered to Enterprise departments. These materials include the ISO "Guidelines for Information Security and Internet Usage", the Federal Trade Commission's "Safe at Any Speed" and "Identity Theft" guides, and password help sheets, all of which are designed to be beneficial both in the work place and at home. If you or your department would like to obtain some of these free documents contact Security Awareness.

Policies, Guidelines, and Procedures

You can find a complete list of Enterprise and DAS-IT security policies, guidelines and procedures, as well as great industry guidelines at http://www.itd.state.ia.us/security/reading.html.

Return to Table of Contents

Upcoming Classes and Consultations

This is the place to learn more about information sharing, security training, conferences, programs, and security vendor announcements.

The Information Security Office's Lunch &Learn Program continues. These informal meetings cover a variety of security-oriented issues. No sign-up or registration is necessary, just drop in. Change of location or time will be announced via e-mail, and sent to departmental Information Security Officer contacts.

Planned Future Sessions Include:

- Home Security for Parents
- New Policies and Policy Creation
- Data Removal – Keeping IT Clean

An updated schedule and past presentations (lots of them - in .pdf, .ppt, and/or video) are available at the Lunch & Learn site.

Please remember - we'll supply the place and the topic, but you will need to bring your own lunch. Questions or topic ideas on the Lunch & Learn program can be directed to William Hubbard.

ITD's Knowledge Access has Security-related training available. Courses available include security topics related to MS Windows 2000, MS IIS 4.0, Network Essentials, Java, and more. Visit the Knowledge Access site for more details and pricing info.

Security Vendors

SANS Offerings:
Each month SANS offers at least one training conference in a major U.S. city. See: http://www.sans.org/SANS2003

SANS also offers online and onsite security courses for those who are unable to travel much, but still wish to participate. Visit http://www.sans.org/newlook/home.php for more info.

If **State of Iowa employees** are interested in an Enterprise-shared SANS session, drop a note to Security Awareness, and note your specific interest, if known (Security Essentials, Securing Windows, Auditing, etc.). If there is enough response the ISO may be able to organize a reduced-cost session specifically for state employees. SANS often can arrange a special on-site session for a reduced cost. Details: http://www.sans.org/onsite

SANS next free Webcast: July 24, 2003

Thursday Tool Talk: Wireless – The Ever Changing Landscape of Network Security
Also – August 6, 2002: Tools and Tips for Analyzing Malware

Check this and others out at: http://www.sans.org/webcasts/

Microsoft: (Vendor Announcements)

Free MSDN Webcasts

Microsoft offers free 90-minute live, interactive webcasts on a variety of topics, including security. Customers can see code and application demos online, and ask the presenter technical questions, or listen to their peers ask questions.
Register at: http://www.microsoft.com/usa/webcasts/upcoming/default.asp
Recorded sessions can be found at:
http://www.microsoft.com/usa/webcasts/ondemand/default.asp.

Microsoft Online Training
Microsoft offers online training for a number of their products. Government workers also get discounts. To register for a course, or just to check them out, visit their website:
http://www.msgovernmenttraining.com/offer/

Other Events:

Defcon 11
Date: August 1-3, 2003
Location: Alexis Park, Las Vegas, NV

A yearly security "get together" of security professionals and enthusiasts. Activities range from hacking and security contests, to speakers and research presentations.

2nd Global Conference War & Virtual War
Date: July 24-27, 2003
Location: West Lafayette, IN

This inter-disciplinary and multi-disciplinary conference marks the continuation of a project launched in 2002 to provide a challenging forum for the examination and evaluation of the nature, purpose and experience of war, and its impacts on all aspects of communities across the world. Viewing war as a multi-layered phenomenon, the conference series seeks to explore the historical, legal, social, religious, economic, and political contexts of conflicts, and assess the place of art, journalism, literature, music, the media and the internet in representation and interpretation of the experience of warfare.

Other notable events in the month of April:
http://security.ittoolbox.com/events/event_body.asp?c=Security_Press&r=http%3A%2F%2Fsecurity%2Eittoolbox%2Ecom%2Fevents%2Fevent%5Fbody%2Easp
Yearly calendar hosted by ITToolbox

Return to Table of Contents

Helpful Hints

Tips On Creating Tough To Hack Passwords (but are easy to remember)

Everyone has heard that they should avoid using bad or easy passwords, but what does that mean. And if you do choose a password that good and tough to hack, how in the world do you remember it? Well here are a few hints, tips and pointers on how to create a strong password.

First of all, what are bad or easy passwords? Well, a bad password is one that is relatively easy to guess. For example: your name, a pet's name, a spouse's name, or even your name spelled backwards. When a cyber criminal attempts to get your password, undoubtedly the first thing they will attempt is the obvious, easy-to-remember words that are all too often used! Choices like god, secret and password are all amazingly poor passwords because they have been commonly used for many years.

Another bad password selection is a word from the dictionary. Why are dictionary words poor choices? Cyber criminals use fast programs that will guess your password by running through every word in the dictionary and plugging them in as your password. If your password is in that dictionary, they can hack it with very minimal effort in a very short time -usually within seconds.

So now we have a very basic idea of what makes a password poor, but what makes it good? There are a few easy methods of creating strong, quality passwords that will be easy to remember.

The first method is the acronym method. Think of a poem, song or saying that you're familiar with. Try to select something that is particularly memorable to you. Then use the first letter of the first few words to make your password. For example, with the phrase "I think therefore I am" could easily become the password ITTFIA. Even better is to mix the case of the letters, and use numbers as well. With this method the phrase could become the password Itt4Ia.

A second method of creating a strong password is to use wild card characters randomly throughout your password. For example the password FREEDOM would be slightly stronger if it were FREED*M!. Although a bit more complicated to remember, it does increase the password's strength. The more varied the characters in a password are, the longer it will take to guess or crack it.

Yet another method is the unique spelling method. One example of this method is Dan Quayle's unique spelling of the word potato. By simply adding an 'e' to the end the word is no longer in the dictionary, and become slightly more difficult to guess. Yet cracking programs can still sometimes get these passwords fairly quickly. Other strong unique spellings include using the phonetic spelling of a word, or spelling a word the way a child or grandchild may have said it while growing up.

Perhaps the strongest method is a combination of some of the above. For example, combining the acronym method, the number method, and the wild character method you may have the phrase "Four score and seven years ago", which could easily become the password "4sc0re7y3ar$!". This combination selection method not only ensures the password is not in the dictionary, but makes in nearly impossible to just guess. This type of password complexity is often required within security-conscious organizations.

So, now with a better idea of how to avoid bad passwords and how to create stronger, yet easy-to-remember new passwords, remember that it is also a good idea to change your password every 60 days. That way if some one does get your password file and tries to crack it, it will be worthless to them within a fairly limited time.

~Doug Houghton
ITD Intern 2003

Return to Table of Contents

Linked Articles

Featured Link

The ABCs of Security
Information security is the process of protecting data from accidental or intentional misuse by persons inside or outside of an organization, including employees, consultants, and yes, the much-feared hacker… And because your risks and vulnerabilities are constantly changing, security is a never-ending process, not something you do once and then forget about. CIO Magazine

Helpful Security Guides

Top 75 Security Tools
A collection of the "Top 75 Security Tools" covering a range of operating systems Updated July 2, 2003, Insecure.org

A Dictionary For Vulnerabilities
CVE gives users, vendors, and toolmakers a common vocabulary for vulnerabilities. June 23, 2003, Ziffdavis

CIO Cyberthreat Response & Reporting Guidelines
CIO worked with the Secret Service, the FBI and industry leaders to create guidelines for reporting security incidents. (PDF.) 7/03, CIO

ZDNet Series: You've been hacked
You've been hacked: What to do first
What should you do in the first five minutes after you discover your system has been hacked?

You've been hacked: What to do in the first hour
What you do in the first hour after a hack attack can make a big difference to the ongoing security of your network - here are the most important steps to take.

You've been hacked: Now prevent future attacks
We have already shown you what to do immediately following a hacker attack, now we will look at some longer term measures to prevent a future attacks.
ZDNet UK, May-July 2003

Penetration Testing for Web Applications (Part Two)
Our first article in this series covered user interaction with Web applications and explored the various methods of HTTP input that are most commonly utilized by developers. In this second installment we will be expanding upon issues of input validation - how developers routinely, through a lack of proper input sanity and validity checking, expose their back-end systems to server-side code-injection and SQL-injection attacks. We will also investigate the client-side problems associated with poor input-validation such as cross-site scripting attacks. July 3, 2003, Security Focus

Education

Computer Security is For Managers, Too
Computer security isn't just an IT headache, say HBS professor Robert D. Austin and co-author Christopher A.R. Darby. Here are eight to-do items for managers to protect their digital assets.
Source: June 30, 2003, Working Knowledge

Program focuses on security response
The Computer Emergency Response Team (CERT) Coordination Center, a security-incident clearinghouse, introduced on Monday a program to certify information technology professionals in incident handling and response. The certification program will train participants in how to react to security incidents and network intrusions. July 14, 2003, ZDNet

Waiting for the Worms
The hole's been announced, the patch has been released. Now there's nothing to do but wait for the worm to come and wreak its ugly havoc. July 21, 2003, Security Focus

Privacy and Security: Finding a Balance
Over the past year and a half, the tug of war between privacy and security has reached a new level, and I'm not convinced that people are willing to give up their privacy in pursuit of security… 04/29/03, PC Magazine

Identity Management
For leaders in the public sector, the emerging debate over identity management and the selections of technology to authenticate citizens and business will be among the most important of all matters to shape the coming information age. NECCC (pdf)

Bug out
This article outlines the value of antivirus software, and how to utilize it to maximize your protection. The article further explains the most common threats to the security of your computer, including worms, Trojans, and logic bombs. June 9, 2003, GCN

Vmyths Hovering At Death's Door
One of the Web's best FUD-fighting sites (Fear, Uncertainty, and Doubt) may not be around much longer. But barring a miracle of the financial sort, Vmyths, which draws thousands of visitors a day, may soon be all but dead. July 3, 2003, Wired News

IDS Correlation of VA Data and IDS Alerts
The sky is falling! The sky is falling! Okay, well the sky isn't really falling, but isn't that they way that we all felt the first time we installed a NIDS and turned it on? June 30, 2003, Security Focus

Report: Many Companies Lack Wi-Fi Security

In a rush to improve productivity, many enterprises have overlooked the need to secure the flow of data over their wireless local area networks (define), according to new research from Jupitermedia's research arm. June 26, 2003, Internetnews.com

Securing PHP: Step-by-step
This article shows the basic steps in securing PHP, one of the most popular scripting languages used to create dynamic web pages, and is a follow-up on the topic of securing an Apache web server. June 23, 2003, Security Focus

Defensive Postures
Intrusion prevention systems offer the latest countermeasures in the war against hackers, worms and viruses. June 15, 2003, CIO Magazine

NIST IR 7007 - An Overview of Issues in Testing Intrusion Detection Systems (PDF)
A discussion regarding comprehensive testing of IDS systems including performance measurements and present difficulties associated with such testing. June 2003, NIST

Cisco warns of DoS flaw in switches
Cisco is warning of a denial of service attack that affects certain models of switches in its Catalyst 4000, 5000 and 6000 lines. July 11, 2003, ITToolbox

Secrets to the best passwords
The use of good, hard-to-guess passwords can make it difficult for a malicious hacker to break into your computer account. Avoiding predictable keywords and using different methods to introduce variety into your passwords makes it easy for you to remember them but virtually impossible for others to guess them. July 14, 2003, Computer World

Spam Believed to Cost Businesses Billions
In addition to being annoying, e-mailed spam costs American businesses billions of dollars in lost time, productivity and e-business as it reduces consumer confidence in the Internet, officials told lawmakers Tuesday. July 9, 2003, Washington Post

E-commerce special report: Security
There are some simple steps every company can take towards ensuring it is protected not only against hackers and fraudsters, but also against charges of negligence when the worst does happen. July 7, 2003 ZDNet UK

Is Intrusion Detection a Dead-End Technology?
A month ago, a Gartner research report declared that intrusion detection systems were a market failure. July 2003, CSO In this Talk Back session, a number of security professionals disagree with Gartner's analysis.

Homeland Security

Senate Blocks Funding for Computer Dragnet

The U.S. Senate voted on Thursday to cut off funding for a widely criticized computer-surveillance program that would comb travel records, credit-card bills and other private records to sniff out suspected terrorists. July 17, 2003, Washington Post

Illinois supercomputer center to head military cybersecurity
Hoping to thwart hackers, the military is launching a new research effort at the University of Illinois to improve the security of battlefield computers and communications systems. Officials at the school\'s National Center for Supercomputing Applications on Thursday announced an initial $5.7 million grant from the Office of Naval Research to establish a new research center to develop technology against enemy hackers, NCSA director Dan Reed said. July 3, 2003, SecurityFocus

Gen. Clark wants more proactive government role in cybersecurity
Retired supreme allied commander Gen. Wesley K. Clark said today that the insurance industry and tougher government enforcement of security standards are keys to improved cybersecurity and critical-infrastructure protection. June 30, 2003, Computer World

First Infragard Conference To Open
Power plants, bridges and buildings aren't the only things vital to national security, computer networks also are crucial. And the FBI can't keep an eye on everything. So a unique partnership called the Infragard program has developed between the FBI and 8,300 companies to share information about both cyber and physical threats. On Monday, experts from around the country were expected to gather for the program's first national conference in Washington, D.C. Some 1,500 people were expected to attend the three-day meetings. June 23, 2003, Hoovers.com

Securing Cyberspace: A Shared Duty
Old equipment, poor practices, slow response blamed for sloppy security. July 15, 2003, Computer World

Lawmakers see cyberterror vulnerability
Lawmakers are charging that government agencies and industry are not doing enough to protect the country’s power plants, industries and financial institutions from the threat of cyberterrorism attacks. 05/28/03, The Hill

Planned U.S. sensor network targets terror threats
Against the backdrop of the war on terrorism, an expanding group of government researchers is at work on a nationwide sensor network that someday could provide a real-time early-warning system for a wide array of chemical, biological and nuclear threats across the United States. July 14, 2003, EETimes

Cyber Crime

Carders are Getting Bold
Credit card fraud "power users" with programming skills and no fear are making it easier for newbies to break into white collar crime, according to a report from the Honeynet Research Alliance this week. The report draws on data gathered earlier this year when a

fraudster looking for a random host to put between himself and IRC wound up cracking a research honeypot maintained by students and faculty at Azusa Pacific University, as part of a loosely affiliated gaggle of deliberately hackable hosts and networks organized around the non-profit Honeynet Project. July 14, 2003, SecurityFocus

FBI fights cybercrime rise
This article provides a strong statistical overview of the growing problem of cyber crime in the United States. The article focuses mainly on Hawaii. May 28, 2003, Honolulu Advisor

Georgia Tech: "Honeypots" catch hackers
The Georgia Institute of Technology has used so-called honeypots to detect 16 compromised systems on the university\'s network in the past six months, security researchers revealed in a paper published online. July 1, 2003, C/Net News.com

Cyberthieves win in online auctions with escrow scam
Sophisticated scam artists are ripping off hundreds of online auction buyers and sellers through bogus escrow services in the latest variation of Internet fraud. July 1, 2003, Seattle Times

Bill would require companies to notify customers when accounts are hacked
Embarrassed businesses and government agencies would have to notify consumers under a proposed law if hackers break into computers and steal some types of personal information, including Social Security numbers, driver\'s license numbers and credit card information. June 27, 2003, SecurityFocus

Fighting the New Face of SPAM
Spam, or junk e-mail is on the rise again, clogging the arteries of networks and servers and sending the blood pressure of many administrators through the ceiling. For effective anti-spam defense, organizations must implement a layered security strategy. 05/02/03, IT Toolbox

Computer security officials discount chances of 'digital Pearl Harbor'
This article discusses the increasing threat of cyber-terrorism, and elaborates on the notion of a “digital Pearl Harbor”. June 3, 2003, Gov Exec

Hackers threaten confidential student records
This article also discusses the rapidly increasing problem of cyber crime. However, this article focuses on high school students, both as victims and perpetrators. May 28, 2003, Santa Cruz Sentinel

Lamo Hacks Cingular Claims Site
Adrian Lamo, a hacker who in the past has broken into The New York Times and Yahoo, found a gaping security hole in a website run by a company that issues the insurance to Cingular customers. By accessing the site, Lamo said he could have pulled up millions of customer records had he wanted to. May 29, 2003, Wired News

Student hackers: we didn't defeat campus debit card system

Two student hackers yesterday settled a lawsuit filed against them by campus debit card firm Blackboard with an admission that they never built a device to defeat the system. July 15, 2003, The Register

MS staffer pleads guilty to $6m software racket
A former Microsoft worker has been caught stealing $6 million of software from Microsoft's internal store in the third case of its type in recent months. July 18, 2003, SecurityFocus

Trojan infection linked to SA Net bank thefts
A Trojan infection has been linked to the theft of hundreds of thousands of rand from Internet accounts held at South African bank Absa. July 21, 2003, The Register

News

Windows 2000 fixes released
Microsoft on Thursday officially released an update to its Windows 2000 operating system. With Windows 2000 Service Pack 4, the software maker added various security and compatibility fixes and provided support for USB (universal serial bus) 2.0 and for wireless Internet connections. June 26, 2003, C/Net News

Can be downloaded here:
http://www.microsoft.com/windows2000/downloads/servicepacks/sp4/default.asp

Do-Not-Call Registry Begins Today
Consumers angry and frustrated over telemarketing calls can take a significant step toward relief today, as the Federal Trade Commission launches a long-awaited nationwide registry for residents who want to block unsolicited advertising via their home and cellular telephones. June 27, 2003, Washington Post.com

A Quantum Leap in Cryptography
In a dark, quiet room inside the Boston labs of BBN Corp. (VZ), network engineer Chip Elliott is using the laws of physics to build what he hopes will be an unbreakable encryption machine. The system, which sits atop a pink heat-absorption table, is designed to harness subatomic particles to create a hacker-proof way to communicate over fiber-optic networks. July 15, 2003, Business Week Online

Teens tutor FBI in cyber-slang
Teens tutor FBI in cyber-slang; Agents brush up on pop knowledge to catch online predators. June 4, 2003 MSNBC

Hacker Damage Reversal Technology Revealed
The University of Michigan is developing a rollback technology that allows administrators to track all transactions on a system, whether authorized or not, and reverse those transactions when required. May 2003, InfoSec News

Libraries Ponder Filtering Decision

This week's Supreme Court ruling on Internet filters in public libraries raises big questions for officials across the country. June 27, 2003, Washington Post.com

Swappers sprint to cloak identities
The response was predictable. The major file-swapping services are rushing to shield users' identities within weeks of the recording industry announcing plans to sue individuals who trade copyrighted music online. July 14, 2003, ITToolbox

DirecTV dragnet snares innocent techies
In recent months the satellite TV giant has filed nearly 9,000 federal lawsuits against people who've purchased signal piracy devices. But some of those devices have legitimate uses, and innocent computer geeks are getting caught in the crackdown. July 17, 2003, Security Focus

Return to Table of Contents

Points of Contact

Pat Clark: DAS ITE Security Supervisor
515-281-7649

Larry Brennan: Critical Infrastructure Assurance Coordinator, Iowa Crisis Action Team
515-281-4436

Adam Kaufman: Security Operations
515-281-4805

William Hubbard: Security Operations, Security Awareness
515-281-5816

Wes Hunsberger: Business Continuity, Physical Security
515-725-0361

Return to Table of Contents

Links to Resources

http://www.itd.state.ia.us/security/
The awesome Enterprise Security website. You can find tons of state or DAS ITE security information here. Policies, procedures, guidelines, educational resources, lists of services, useful links, and more!

http://www.cert.org/nav/index.html
Homepage for CERT (Computer Emergency Response Team)

http://www.sans.org/newlook/home.htm

SANS (System Administration, Networking, and Security)

FBI and SANS List Top 20 Vulnerabilities

The FBI's NIPC and the SANS Institute published a revised list of the top twenty Internet security vulnerabilities along with instructions on how to fix them.

Iowa Homeland Security

This site includes much information about Iowa's Homeland Security Initiatives, Press Releases, Preparedness Information, and more. Includes the final version of the Iowa Homeland Security Initiative.

Stay Safe Online

A site dedicated to educating citizens and helping them to secure their home systems. Sponsored by the National Cyber Security Alliance.

Return to Table of Contents

If you have questions or comments relating to this newsletter, or if there is a topic you would like to see an article on, please contact William Hubbard.

The ISO Code:

Integrity…Service…Excellence